

The University of Chicago

DIVISION ALGEBRAS DEFINED BY
NON-ABELIAN GROUPS

A DISSERTATION SUBMITTED TO THE
FACULTY OF THE DIVISION OF THE
PHYSICAL SCIENCES IN CANDIDACY FOR
THE DEGREE OF DOCTOR OF PHILOSOPHY

DEPARTMENT OF MATHEMATICS

1936

By

DORA McFARLAND

Private Edition, Distributed by
THE UNIVERSITY OF CHICAGO LIBRARIES
CHICAGO, ILLINOIS

1936

The University of Chicago

**DIVISION ALGEBRAS DEFINED BY
NON-ABELIAN GROUPS**

A DISSERTATION SUBMITTED TO THE
FACULTY OF THE DIVISION OF THE
PHYSICAL SCIENCES IN CANDIDACY FOR
THE DEGREE OF DOCTOR OF PHILOSOPHY

DEPARTMENT OF MATHEMATICS

1936

By

DORA McFARLAND

Private Edition, Distributed by
THE UNIVERSITY OF CHICAGO LIBRARIES
CHICAGO, ILLINOIS

1936



TABLE OF CONTENTS

1.	INTRODUCTION - - - - -	page 1
	a. Historical	
	b. Classification of groups of order < 48	
	c. Statement of problem	
2.	THE GROUP G - - - - -	page 2
	a. Definition	
	b. Laws of operation	
	c. Derived congruences	
3.	THE SUBALGEBRA Σ AND THE ALGEBRA Γ - - -	page 6
4.	ASSOCIATIVITY CONDITIONS FOR Γ - - - -	page 7
	a. $A'B' = (AB)'$ obtained by means of equations (32), (33), (34) - - -	page 7
	b. $\gamma' = \gamma$ obtained by means of equation (35) - - - - -	page 18
	c. $A^{(P_2)} = \gamma A \gamma^{-1}$ obtained by means of equations (47), (48) - - -	page 18



Digitized by the Internet Archive
in 2026

https://archive.org/details/IA41548411_0021

1. INTRODUCTION.

The treatment of problems concerning division algebras has covered a considerable period of years. It began with the announcement¹ in 1905 by Professor L. E. Dickson of his discovery of a division algebra D of order n^2 over a field F . In a later paper² he has shown how to construct all algebras Γ of order $n^2 = Q^2 q^2$ over a field F , corresponding to the solvable Galois group G of order $n = Qq$ of an equation $f(x) = 0$, irreducible in F and having all its roots rational functions of one root with coefficients in F . Dickson has also given the general conditions which must be satisfied by the algebra Γ if it is associative. Since then Williamson³ has given these conditions in more detail for an algebra corresponding to a solvable Galois group G when G has two generators. He also treated a special case of the three-generator problem, but without the benefit of a later simplification⁴ of the two-generator problem by Dickson.

Based upon this work, it is our problem to obtain the conditions for associativity of an algebra Γ corresponding to a solvable group G with three generators, ψ_1, ψ_2, ψ_3 .

Upon investigation⁵ it was found that all the groups of

-
1. Bulletin of the American Mathematical Society, Vol. 22, (1905-06), p. 442.
 2. New Division Algebras, Transactions of the American Mathematical Society, Vol. 28, (1926), pp. 207-34.
 3. Associativity of Division Algebras, Transactions of the American Mathematical Society, Vol. 30, (1928), pp. 111-25.
 4. Transactions of the American Mathematical Society, Vol. 32, (1930), pp. 319-34.
 5. Miller, Number of Distinct Regular Groups of Order $r < 48$, Quarterly Journal of Pure and Applied Mathematics, Vol. 28, (1896), p. 232; LeVavasseur, Enumeration des groupes d'opérations d'ordre donné.

order < 48 (omitting order 32, which was not examined, and one group of order 24, which requires four generators) are abelian or belong to the two-generator type mentioned above except, perhaps, those given below. Each group is of order $p_1 p_2 p_3$, and has the three generators ψ_1, ψ_2, ψ_3 , which obey the laws:

$$\begin{aligned} \psi_2^{-1} \psi_1 \psi_2 &= \psi_1^x, & \psi_3^{-1} \psi_1 \psi_3 &= \psi_2^v \psi_1^y, & \psi_3^{-1} \psi_2 \psi_3 &= \psi_2^z \psi_1^w, \\ \psi_1^{p_1} &= 1, & \psi_2^{p_2} &= \psi_1^c, & \psi_3^{p_3} &= \psi_2^{e_2} \psi_1^{e_1}, \end{aligned}$$

where the letters, $p_1, p_2, p_3, x, v, y, z, w, c, e_1, e_2$, take the values in the table.

p_1	2	4	4	4	4	3	4	6	2	3	3	6	6	6	6	3	3	10	10	10
p_2	2	2	2	2	2	3	2	2	2	4	3	2	2	3	3	6	3	2	2	2
p_3	3	2	2	2	2	2	3	2	6	2	3	3	3	2	2	2	4	2	2	2
x	1	1	1	1	1	1	3	5	1	2	1	1	1	1	1	2	1	1	1	1
v	1	0	0	0	1	0	1	0	1	0	0	1	1	0	0	0	1	1	0	0
y	0	1	3	3	0	2	3	1	0	1	1	0	0	5	5	2	1	4	9	9
z	1	1	1	1	0	2	0	1	1	3	1	1	1	2	2	5	2	0	1	1
w	1	2	2	2	1	0	1	0	1	0	1	3	3	3	3	1	1	5	0	0
c	0	0	2	2	2	0	2	0	0	0	0	2	2	3	3	0	0	0	0	0
e_1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	3	0	0	0	5
e_2	0	0	0	2	0	0	0	0	0	0	0	0	0	2	0	0	0	0	0	0

Incidentally, this shows the existence of the various types of groups to which our investigation applies.

2. THE GROUP G.

Let the group G, which is not necessarily abelian, have three generators ψ_1, ψ_2, ψ_3 , which obey the laws:

$$(1) \quad \psi_2^{-1} \psi_1 \psi_2 = \psi_1^x, \quad \psi_3^{-1} \psi_1 \psi_3 = \psi_2^y \psi_1^y, \quad \psi_3^{-1} \psi_2 \psi_3 = \psi_2^z \psi_1^w,$$

(x, y, w integers ≥ 0 and $< p_1$; v, z integers ≥ 0 and $< p_2$),

and

$$(2) \quad \psi_1^{p_1} = 1, \quad \psi_2^{p_2} = \psi_1^c, \quad \psi_3^{p_3} = \psi_2^{e_2} \psi_1^{e_1},$$

$$(0 < p_1, e_1 < p_1, e_2 < p_2).$$

Then it is easily shown that

$$(3) \quad \psi_2^{-s} \psi_1^h \psi_2^s = \psi_1^{hx^s},$$

$$(4) \quad \psi_3^{-1} \psi_1^h \psi_3 = \psi_2^{hv} \psi_1^{\sum_{i=0}^{h-1} yx^{iv}},$$

$$(5) \quad \psi_3^{-1} \psi_2^h \psi_3 = \psi_2^{hz} \psi_1^{\sum_{i=0}^{h-1} wx^{iz}},$$

Where h and s are integers > 0 . We may prove by induction that

$$(6) \quad \psi_3^{-s} \psi_1 \psi_3^s = \psi_2^{a_s} \psi_1^{b_s},$$

where

$$a_1 = v, \quad b_1 = y,$$

$$a_k = a_{k-1}z + b_{k-1}v,$$

$$b_k = x^{b_{k-1}v} \sum_{i=0}^{a_{k-1}-1} wx^{iz} + \sum_{i=0}^{b_{k-1}-1} yx^{iv};$$

and, likewise, that

$$(7) \quad \psi_3^{-s} \psi_2 \psi_3^s = \psi_2^{f_s} \psi_1^{d_s},$$

where

$$f_1 = z, \quad d_1 = w,$$

$$f_k = f_{k-1}z + d_{k-1}v,$$

$$d_k = x^{d_{k-1}v} \sum_{i=0}^{f_{k-1}-1} wx^{iz} + \sum_{i=0}^{d_{k-1}-1} yx^{iv}.$$

We shall employ, throughout this discussion, the symbols $[x]_1$, $[x]_2$ to denote the least positive residues of any number x , modulo p_1 and p_2 , respectively. Also, $\{x\}_1$, $\{x\}_2$ shall denote the corresponding largest quotients when x is divided by p_1 and p_2 . To illustrate, the symbols satisfy the relations:

$$x = \{x\}_1 p_1 + [x]_1, \quad x = \{x\}_2 p_2 + [x]_2.$$

We note that

$$[[x]_1 + [y]_1]_1 = [x+y]_1,$$

and

$$[[x]_1, [y]_1]_1 = [xy]_1.$$

The same statements are true of symbols relating to the modulus p_2 .

The statements, (1)-(7), may be used to derive certain congruences. From (3) with $s = kp_2$ we get

$$(8) \quad h \equiv hx^{kp_2} \pmod{p_1};$$

while if, instead, we let $h=c$, then

$$(9) \quad c \equiv cx^s \pmod{p_1}.$$

Since the transforms of ψ_1^c and $\psi_2^{p_2}$ by ψ_3 are equal,

$$(10) \quad \left\{ \begin{array}{l} p_2 z - cv \equiv 0 \pmod{p_2}, \\ \{p_2 z - cv\}_2 c + \sum_{i=0}^{p_2-1} wx^iz - \sum_{i=0}^{c-1} yx^iv \equiv 0 \pmod{p_1}. \end{array} \right.$$

Similarly, since the transforms of $\psi_3^{p_3}$ and $\psi_2^{e_2} \psi_1^{e_1}$ by ψ_3 are equal,

$$(11) \quad \left\{ \begin{array}{l} e_2 z + e, v - e_2 \equiv 0 \quad (\text{mod } p_2), \\ \{e_2 z + e, v - e_2\}_2 \alpha + x^{e_1 v} \sum_{i=0}^{e_2-1} w x^{i z} + \sum_{i=0}^{e_1-1} y x^{i v} - e \equiv 0 \quad (\text{mod } p_1). \end{array} \right.$$

If in (6) we put $s=p_3$ and use (22) as before, we get

$$(12) \quad \left\{ \begin{array}{l} a_{p_3} \equiv 0 \quad (\text{mod } p_2), \\ \{a_{p_3}\}_2 \alpha + b_{p_3} - x^{e_1} \equiv 0 \quad (\text{mod } p_1). \end{array} \right.$$

Similarly (7) with $s=p_3$ yields

$$(13) \quad \left\{ \begin{array}{l} f_{p_3} - 1 \equiv 0 \quad (\text{mod } p_2), \\ \{f_{p_3} - 1\}_2 \alpha + e, x^{f_{p_3}} + d_{p_3} - e \equiv 0 \quad (\text{mod } p_1). \end{array} \right.$$

Next we make use of the identity

$$\psi_3^{-1} (\psi_2^{-1} \psi_1 \psi_2) \psi_3 = (\psi_2 \psi_3)^{-1} \psi_1 (\psi_2 \psi_3)$$

We replace $\psi_2 \psi_3$ by its value from (13); replace the left member $\psi_3^{-1} \psi_1^k \psi_3$ by its value from (4); multiply both members on the left by ψ_1^w ; and, finally, replace $\psi_1^w \psi_2^{xv}$, which occurs in the left member, by its value from (3). From this we see that

$$(14) \quad \left\{ \begin{array}{l} xv - v \equiv 0 \quad (\text{mod } p_2), \\ \{xv - v\}_2 \alpha + wx^{xv} + \sum_{i=0}^{x-1} y x^{i v} - w - y x^z \equiv 0 \quad (\text{mod } p_1). \end{array} \right.$$

It follows from (4) with $h = p_1$ that

$$(15) \quad \begin{cases} p_1 v \equiv 0 & (\text{mod } p_2), \\ \{p_1, v\}_2 c + \sum_{i=0}^{p_1-1} y x^{iv} \equiv 0 & (\text{mod } p_1). \end{cases}$$

3. THE SUBALGEBRA Σ AND THE ALGEBRA Γ .

In accordance with the theory developed on pages 211-2 of the paper, New Division Algebras¹, we may write

$$(16) \quad j_1 \cdot i = \psi_1 j_1, \quad j_2 \cdot i = \psi_2 j_2, \quad j_3 \cdot i = \psi_3 j_3,$$

$$(17) \quad j_1^{p_1} = g, \quad j_2^{p_2} = \rho j_1^c, \quad j_3^{p_3} = \sigma j_1^{e_1} j_2^{e_2},$$

$$(18) \quad j_2 j_1 = \beta j_1^x j_2, \quad j_3 j_1 = \alpha j_1^y j_2^v j_3, \quad j_3 j_2 = \delta j_1^w j_2^z j_3,$$

where $\psi_1, \psi_2, \psi_3, g, \rho, \sigma, \beta, \alpha, \delta$ are functions of i , and where i, j_1, j_2, j_3 generate the algebra Γ . From (16) it follows that

$$(19) \quad \begin{aligned} j_1^r f(i) &= f(\psi_1^r) j_1^r, & j_2^r f(i) &= f(\psi_2^r) j_2^r, \\ j_3^r f(i) &= f(\psi_3^r) j_3^r, \end{aligned}$$

where $\psi_k^r(i)$ is the r -th iterative of the function $\psi_k(i)$, ($k=1, 2, 3$). Since the subgroup of G generated by ψ_1, ψ_2 is of the type used in the discussion of the two-generator problem,² we know the conditions for associativity of the subalgebra Σ connected with it and generated by i, j_1, j_2 . Hence we may assume that Σ is associative.

The general element of Γ is defined as

$$A = \sum_k \sum_i f_{ki}(i) j_i^k j^i.$$

1. See note 2, page 1.

2. See notes 3 and 4, page 1.

We also make the definition

$$A' = j_3 A j_3^{-1}.$$

From this it follows at once that

$$(20) \quad i' = \psi_3(i), \quad j_1' = \alpha j_1^y j_2^v, \quad j_2' = \delta j_1^w j_2^z.$$

4. ASSOCIATIVITY CONDITIONS FOR Γ .

We can reduce AB to C by the use of (16₁), (16₂), (17₁), (17₂) and (18₁). AB' can be reduced to C' by the following corresponding relations:

$$(21) \quad j_1' i' = \psi_1(i') j_1', \quad j_2' i' = \psi_2(i) j_2',$$

$$(22) \quad (j_1')^p = g(i'), \quad (j_2')^{p_2} = \rho(i') (j_1')^c,$$

$$(23) \quad j_2' j_1' = \beta(i') (j_1')^x j_2'.$$

These five relations will be discussed in turn.

We may write (21₁) as

$$\alpha j_1^y j_2^v \psi_3(i) = \psi_1(\psi_3) \alpha j_1^y j_2^v,$$

i.e.

$$\alpha \psi_3 [\psi_2^v(\psi_1^y)] = \psi_1(\psi_3) \alpha.$$

Since functions of i are commutative, the α in each member may be cancelled and the condition reduced to

$$\psi_3[\psi_2^v(\psi_1^y)] = \psi_1(\psi_3)$$

This is true from (1₂) since relations between the generators, j_i , of G imply the same relations between the roots ψ_i of the equation. In the same manner (21₂) reduces to

$$\psi_3[\psi_2^z(\psi_1^w)] = \psi_2(\psi_3),$$

which is true by (1₃). Hence the equations (21) yield no new associativity conditions for Γ .

Before discussing (22) and (23), it is necessary to find expressions for the powers of j_1' and j_2' . We first show that

$$(24) \quad j_2 j_1^f = B_1 j_1^{[x]}, j_2,$$

where

$$B_1 = [q(\psi_2)]^{\{f\}} \beta \beta(\psi_1^x) \beta(\psi_1^{[2x]}) \dots \beta(\psi_1^{[(l-1)x]}) q^{\{f\}_1 - x \{f\}},$$

Note that the number of β 's is equal to $[x]_1$. Hence for $[x]_1 = 0$, B_1 reduces to $[q(\psi_2)]^{\{f\}_1}$. The proof which follows is by an induction on x . If we multiply on the right by j_1 , we get

$$j_2 j_1^{f+1} = B_1 \beta(\psi_1^{[fx]}) q^{\{[x]_1 + x\}_1} j_1^{[fx]_1 + x} j_2.$$

We know from the nature of the symbol $[]_1$ that

$$[[x]_1 + x]_1 = [(x+1)x]_1.$$

Hence the exponents of j_1 and j_2 are correct for the induction.

We have yet to show that

$$(25) \quad [q(\psi_2)]^{\{f\}_1} \beta \beta(\psi_1^x) \dots \beta(\psi_1^{[(l-1)x]}) \beta(\psi_1^{[fx]}) q^{\{f\}_1 - x \{f\}_1 + \{[fx]_1 + x\}_1} \\ = [q(\psi_2)]^{\{f+1\}_1} \beta \beta(\psi_1^x) \dots \beta(\psi_1^{[(l+1)x]}) q^{\{[x+1]_1\}_1 - x \{f+1\}_1}.$$

There are two cases to be considered:

Case I. If $\{x+1\}_1 = \{x\}_1$, then $[x+1]_1 = [x]_1 + 1$.

It is evident that in this event the exponents of $g(\psi_2)$ are the same and that the β 's are identical. Also the exponents of g are equal since

$$\{(x+1)x\}_1 = \{x\}_1 + \{[x]_1 + x\}_1$$

follows by adding x to each member of

$$x = \{x\}_1 p_1 + [x]_1.$$

Case II. Let $\{x+1\}_1 = \{x\}_1 + 1$. Then $[x+1]_1 = 0$ and $[x]_1 = p_1 - 1$. It is also evident that

$$[x]_1 = [[x] x]_1 = [(p_1 - 1)x]_1.$$

Since it follows from the associativity conditions for Σ that

$$\beta\beta(\psi, x) \beta(\psi, [2x]_1) \dots \beta(\psi, [(p-1)x]_1) g^x = g(\psi_2),$$

the β 's in the left member of (25) may be omitted and 1 added to the exponent of $g(\psi_2)$. We must remember to subtract x from the exponent of g at the same time. From the remark following the definition of B_f , we know that the right member of (25) is, in this case, simply $g(\psi_2)^{\{f+1\}_1}$. It remains to be shown that the exponent of g ,

$$\{[x]_1\} - x\{f\}_1 + \{[fx]_1 + x\}_1 - x,$$

is zero. This follows at once from the fact that

$$\{[x]_1\} + \{[fx]_1 + x\}_1 = x\{f+1\}_1,$$

since, by hypothesis, the right member can be written as $x(\{f\}_1 + 1)$. Hence the induction is complete.

Now, using (24), we see that

$$j_2^2 j_1^f = B_f(\psi_2) B_{[fx]_1} j_1^{[fx]_1 x} j_2^2.$$

We need to establish a general rule for j_2^k , where $k < p_2$. The formula which we will prove by an induction on k , is

$$j_2^k j_1^f = B_f(\psi_2^{k-1}) B_{[fx]_1} (\psi_2^{k-2}) B_{[fx]_1} (\psi_2^{k-3}) \dots \\ \dots B_{[fx]_1^{k-2}} (\psi_2) B_{[fx]_1^{k-1}} j_1^{[fx]_1^k} j_2^k.$$

After multiplying on the left by j_2 , we have

$$j_2^{k+1} j_1^f = B_f(\psi_2^k) B_{[fx]_1} (\psi_2^{k-1}) \dots B_{[fx]_1^{k-1}} j_2 j_1^{[fx]_1^k} j_2^k \\ = B_f(\psi_2^k) B_{[fx]_1} (\psi_2^{k-1}) \dots B_{[fx]_1^k} j_1^{[fx]_1^k x} j_2^{k+1}.$$

Since $[([fx]_1^k)x]_1 = [fx]_1^{k+1}$, the induction is complete.

If we make the definitions:

$$B_{k,f} = B_f(\psi_2^{k-1}) B_{[fx]_1} (\psi_2^{k-2}) \dots B_{[fx]_1^{k-2}} (\psi_2) B_{[fx]_1^{k-1}}, \\ B_{0,f} = g^{\{f\}_1},$$

then

$$(26) \quad j_2^k j_1^l = B_{k,l} j_1^{[lx^k]}, j_2^k \quad (0 \leq k, p) \quad (l \text{ integer} > 0).$$

In finding an expression for $(j_1')^m$, it is necessary to consider two cases in each step, as the power is built up. This will be clear if we build up $(j_1')^3$ as an illustration.

$$j_1' = \alpha j_1^y j_2^v.$$

$$(j_1')^2 = \alpha \alpha [\psi_2^v(\psi_1^y)] j_1^y j_2^v j_1^y j_2^v.$$

Case I, when $\{[v]_2 + v\}_2 = 0$:

$$(j_1')^3 = \alpha \alpha [\psi_2^v(\psi_1^y)] B_{y,y}(\psi_1^y) g^{\{y+[yx^v]\}_1} \alpha [\psi_2^{[2v]_2}(\psi_1^{[y+yx^v]_1})] j_1^{[y+yx^v]_1} j_2^{[2v]_2} j_1^y j_2^v.$$

Case II, when $\{[v]_2 + v\}_2 = 1$:

$$(j_1')^3 = \alpha \alpha [\psi_2^v(\psi_1^y)] B_{p_2-v,y}[\psi_2^{[2v]_2}(\psi_1^y)] \rho \{ \psi^{[yx^{p_2-v}]_1} [\psi_2^{[2v]_2}(\psi_1^y)] \}$$

$$g^{\{[yx^{p_2-v}]_1 + c + y\}_1} [\psi_2^{[2v]_2}(\psi_1^y)] \alpha \{ \psi^{[yx^{p_2-v}+c]_1} [\psi_2^{[2v]_2}(\psi_1^y)] \}$$

$$j_1^y j_2^{[2v]_2} j_1^{[yx^{p_2-v}+c+y]_1} j_2^v.$$

If $r_{y,1} = 1$ and $\lambda_{y,1} = \frac{[v]_2}{p_2-v}$, according as $S_{y,1} = \{[v]_2 + v\}_1 = 0$, then the two cases can be combined as

$$(j_1')^3 = M_0 M_1 M_2 j_1^{[y+r_{y,1}yx^v]_1} j_2^{[2v]_2} j_1^{[y+S_{y,1}(yx^{p_2-v}+c)]_1} j_2^v,$$

where

$$(27) \quad \left\{ \begin{array}{l} M_0 = \alpha, \\ M_1 = \alpha [\psi_2^v(\psi_1^y)], \\ M_2 = B_{\lambda_{y,1},y} [\psi_2^{S_{y,1}[2v]_2}(\psi_1^y)] \left(\rho \{ \psi^{[yx^{p_2-v}]_1} [\psi_2^{[2v]_2}(\psi_1^y)] \} \right)^{S_{y,1}} \\ \quad g^{\{y+[yx^{\lambda_{y,1}}]_1 + S_{y,1}c\}_1} [\psi_2^{S_{y,1}[2v]_2}(\psi_1^{S_{y,1}[y]_1})] \\ \quad \alpha \{ \psi^{S_{y,1}[yx^{p_2-v}+c]_1} [\psi_2^{[2v]_2}(\psi_1^{[y+r_{y,1}yx^v]_1})] \}. \end{array} \right.$$

In order to make the induction complete for the establishment of a general rule for powers of j_1' , it will be nec-

essary to find $(j'_1)^4$. We will, however, leave it to the reader to work out the two cases as we did for $(j'_1)^3$. The final result is

$$(28) \quad (j'_1)^4 = M_0 M_1 M_2 B_{\lambda_{v,2}, [y+s_{v,1}(yx^{p_2-v}+c)]_1} [\psi_2^{S_{v,2}[3v]_2} (\psi_1^{[y+r_{v,1}, yx^v]_1})] \\ (\rho \{ \psi_1^{[yx^{p_2-v} + s_{v,1}(yx^{p_2-v}+c)]_1} [\psi_2^{[3v]_2} (\psi_1^{[y+r_{v,1}, yx^v]_1})] \}^{S_{v,2}} \\ g \{ [yx^{\lambda_{v,2}} + s_{v,1}(yx^{p_2-v}+c)x^{\lambda_{v,2}}]_1 + r_{v,2}[y+r_{v,1}, yx^v]_1 + s_{v,2}(y+c) \}_1 [\psi_2^{S_{v,2}[3v]_2} (\psi_1^{S_{v,2}[y+r_{v,1}, yx^v]_1})] \\ \alpha \{ \psi_1^{S_{v,2}[yx^{p_2-v} + s_{v,1}(yx^{p_2-v}+c)]_1} [\psi_2^{[3v]_2} (\psi_1^{[y+r_{v,1}, yx^v+r_{v,2}yx^{[2v]_2} + r_{v,2}s_{v,1}(yx^{p_2-v}+c)x^{[2v]_2}]_1})] \} \\ \cdot [y+r_{v,1}, yx^v+r_{v,2}yx^{[2v]_2} + r_{v,2}s_{v,1}(yx^{p_2-v}+c)x^{[2v]_2}]_1 \cdot [3v]_2 \cdot [y+s_{v,2}yx^{p_2-v} + s_{v,2}s_{v,1}(yx^{p_2-v}+c)x^{p_2-v} + s_{v,2}c]_1 \cdot v \\ j_2 \}.$$

The general law for powers of j'_1 , which we will prove by induction, is

$$(29) \quad (j'_1)^m = M_0 M_1 M_2 M_3 \dots M_{m-1} j_1^{[X_{y,m-2}]_1} j_2^{[(m-1)v]_2} j_1^{[T_{y,m-2}]_1} j_2^v,$$

where

$$r_{v,k} = \begin{pmatrix} 1 \\ 0 \end{pmatrix}, \text{ and } \lambda_{v,k} = \begin{pmatrix} [kv]_2 \\ p_2-v \end{pmatrix}, \text{ according as } S_{v,k} = \begin{cases} [kv]_2 + v \\ 0 \end{cases} \begin{pmatrix} 0 \\ 1 \end{pmatrix},$$

$$\eta_{y,k} = (yx^{p_2-v} + c) \sum_{i=0}^k s_{v,i} \sum_{j=i+1}^{k+1} r_{v,j} x^{[jv]_2 + (j-1-i)(p_2-v)} \prod_{f=i}^{j-1} s_{v,f},$$

$$\xi_{y,k} = \sum_{i=0}^k r_{v,i} yx^{[iv]_2}, \quad X_{y,k} = \xi_{y,k} + \eta_{y,k-1},$$

$$J_{y,k} = (yx^{p_2-v} + c) \sum_{i=0}^k x^{(k-i)(p_2-v)} \prod_{f=i}^k s_{v,f}, \quad T_{y,k} = y + J_{y,k},$$

$$W_{y,k} = [T_{y,k} x^{\lambda_{v,k+1}}]_1 + s_{v,k+1}(y+c) + r_{v,k+1} [X_{y,k}]_1,$$

$$M_k = B_{\lambda_{v,k-1}, [T_{y,k-2}]_1} [\psi_2^{S_{v,k-1}[kv]_2} (\psi_1^{[X_{y,k-2}]_1})] (\rho \{ \psi_1^{[T_{y,k-2} x^{p_2-v}]_1}$$

$$[\psi_2^{[kv]_2} (\psi_2^{[X_{y,k-2}]_1})] \}^{S_{v,k-1}} g \{ W_{y,k-2} \}_1 [\psi_2^{S_{v,k-1}[kv]_2} (\psi_1^{S_{v,k-1}[X_{y,k-2}]_1})]$$

$$\alpha \{ \psi_1^{S_{v,k-1}[T_{y,k-2} x^{p_2-v} + c]_1} [\psi_2^{[kv]_2} (\psi_1^{[X_{y,k-2} + r_{v,k-1} T_{y,k-2} x^{[(k-1)v]_2}]_1})] \}.$$

The definitions for M_0 , M_1 , M_2 are given in (27).

If we remember that $s_{y,0} = 0$, and hence $r_{y,0} = 1$, the symbols involved in (29) with $m=4$ take the following meanings:

$$\begin{aligned} X_{y,1} &= \xi_{y,1} + \eta_{y,0} = y + r_{y,1} yx^v, \\ X_{y,2} &= \xi_{y,2} + \eta_{y,1} = y + r_{y,1} yx^v + r_{y,2} yx^{[2v]_2} + (yx^{p_2-v} + c) s_{y,1} r_{y,2} x^{[2v]_2}, \\ T_{y,1} &= y + \eta_{y,1} = y + (yx^{p_2-v} + c) s_{y,1}, \\ T_{y,2} &= y + \eta_{y,2} = y + (yx^{p_2-v} + c) [x^{p_2-v} s_{y,1} s_{y,2} + s_{y,2}], \\ W_{y,1} &= [T_{y,1}, x^{\lambda_{y,1}}]_1 + s_{y,2} (y+c) r_{y,2} [X_{y,1}]_1 = [yx^{\lambda_{y,1}} + s_{y,1} (yx^{p_2-v} + c) x^{\lambda_{y,1}}]_1 + s_{y,2} (y+c) r_{y,2} [y + r_{y,1} yx^v]_1. \end{aligned}$$

When substituted in (29) these values give exactly the same result as (28) which was obtained directly.

To complete the induction:

$$(\mathfrak{J}_i')^{m+1} = M_0 \dots M_{m-1} \mathfrak{J}_1 [X_{y,m-1}]_2 [^{(m-1)v}]_2 \mathfrak{J}_1 [T_{y,m-1}]_1 \mathfrak{J}_2^v \propto \mathfrak{J}_1^y \mathfrak{J}_2^v.$$

As before, the simplification must be carried out in two cases and afterwards combined.

Case I, when $\{[(m-1)v]_2 + v\}_2 = 0$:

$$\begin{aligned} (\mathfrak{J}_i')^{m+1} &= M_0 \dots M_{m-1} \mathfrak{B}_{[^{(m-1)v}]_2, [T_{y,m-1}]_1} (\psi_1 [X_{y,m-2}]_1) \\ &= q \{ [X_{y,m-2}]_1 + [T_{y,m-2} x^{[(m-1)v]_2}]_1 \} \alpha \{ \psi_z [mv]_z (\psi_1 [X_{y,m-1} + T_{y,m-2} x^{[(m-1)v]_2}]_1) \} \\ &= \mathfrak{J}_1 [X_{y,m-2} + T_{y,m-2} x^{[(m-1)v]_2}]_1 \mathfrak{J}_2 [mv]_z \mathfrak{J}_1^y \mathfrak{J}_2^v. \end{aligned}$$

Case II, when $\{[(m-1)v]_2 + v\}_2 = 1$:

$$\begin{aligned} (\mathfrak{J}_i')^{m+1} &= M_0 \dots M_{m-1} \mathfrak{B}_{p_2-v, [T_{y,m-2}]_1} [\psi_z^{[mv]_2} (\psi_1 [X_{y,m-2}]_1)] \\ &= \rho \{ \psi_1 [T_{y,m-2} x^{p_2-v}]_1 [\psi_z [mv]_z (\psi_1 [X_{y,m-2}]_1)] \} q \{ [T_{y,m-2} x^{p_2-v}]_1 + c + y \} \psi_z [mv]_z \\ &= (\psi_1 [X_{y,m-2}]_1) \alpha \{ \psi_1 [T_{y,m-2} x^{p_2-v} + c]_1 [\psi_z [mv]_z (\psi_1 [X_{y,m-2}]_1)] \} \\ &= \mathfrak{J}_1 [X_{y,m-2}]_1 \mathfrak{J}_2 [mv]_z \mathfrak{J}_1 [T_{y,m-2} x^{p_2-v} + c + y]_1 \mathfrak{J}_2^v. \end{aligned}$$

To combine cases use

$$\lambda_{v,m-1} = \frac{[(m-1)v]_2}{p_2-v}, \text{ and } r_{y,m-1} = \frac{1}{0}, \text{ according as } s_{y,m-1} = \{[(m-1)v]_2 + v\}_2 \stackrel{!}{=} 0.$$

Then

$$\begin{aligned}
 (j_1')^{m+1} &= M_0 \dots M_{m-1} B_{\lambda_{y,m-1}, [\tau_{y,m-2}]_1} [\psi_2^{S_{y,m-1} [mv]_2} (\psi_1^{[X_{y,m-2}]_1})] \\
 &\left(\rho \left\{ \psi_1^{[\tau_{y,m-2} X^{p_2-v}]_1} [\psi_2^{[mv]_2} (\psi_1^{[X_{y,m-2}]_1})] \right\} \right)^{S_{y,m-1}} g \left\{ r_{y,m-1}^{[mv]_2} [\psi_1^{[X_{y,m-2}]_1} + [\tau_{y,m-2} X^{p_2-v}]_1 + S_{y,m-1} (y+c)] \right\}_1 \\
 &[\psi_2^{S_{y,m-1} [mv]_2} (\psi_1^{S_{y,m-1} [X_{y,m-2}]_1})] \alpha \left\{ \psi_1^{S_{y,m-1} [\tau_{y,m-2} X^{p_2-v} + c]_1} [\psi_2^{[mv]_2} (\psi_1^{[X_{y,m-2} + r_{y,m-1} \tau_{y,m-2} X^{[m-1]v]_2})] \right\} \\
 &\cdot \frac{[X_{y,m-2} + r_{y,m-1} \tau_{y,m-2} X^{[m-1]v}]_1 \cdot [mv]_2}{j_2} \cdot \frac{[S_{y,m-1} (\tau_{y,m-2} X^{p_2-v} + c) + y]_1}{j_1} \cdot \frac{v}{j_2} .
 \end{aligned}$$

Since the factors from B to α , inclusive, are exactly M_m , the induction will be complete if we show that the exponents of j_1 are correct, i.e. that

$$X_{y,m-2} + r_{y,m-1} \tau_{y,m-2} X^{[m-1]v} = X_{y,m-1} ,$$

and

$$S_{y,m-1} (\tau_{y,m-2} X^{p_2-v} + c) + y = \tau_{y,m-1} .$$

Substituting from the values given in (29), the first statement to be proved becomes

$$\xi_{y,m-2} + \eta_{y,m-3} + r_{y,m-1} (y + j_{y,m-2}) X^{[m-1]v} = \xi_{y,m-1} + \eta_{y,m-2} .$$

We see at once from the definitions of these symbols that

$\xi_{y,m-2} + r_{y,m-1} y X^{[m-1]v}$ make up $\xi_{y,m-1}$, while the remaining terms, $\eta_{y,m-3} + r_{y,m-1} X^{[m-1]v} j_{y,m-2}$, may be recombined and produce $\eta_{y,m-2}$. It is not at all difficult, by the use of these same definitions, to establish the second statement as well.

The next step in the simplification of $(j_1')^m$ is the combining of the two factors which are powers of j_1 and the two which are powers of j_2 into a single factor each. This last step, in contrast to all which have preceded it, is carried out completely, regardless of the value of $\{(m-1)v\}_2 + v\}_2$. After the completion of this step we can say that

$$(j_1')^m = M_0 M_1 \dots M_{m-1} \bar{M}_{m-1} j_1^{[X_{y,m-2} + \tau_{y,m-2} X^{[m-1]v} + S_{y,m-1} c]_1} j_2^{[mv]_2} ,$$

where

$$\bar{M}_{m-1} = B_{[m-1]v]_2, [T_{y, m-2}]_1} (\psi, [X_{y, m-2}]_1) g \left\{ [X_{y, m-2}]_1 + [T_{y, m-2} X^{[(m-1)v]_2}]_1 + S_{y, m-1} c \right\}, \\ (\rho(\psi, [X_{y, m-2} + T_{y, m-2} X^{[(m-1)v]_2}]_1))^{S_{y, m-1}}.$$

It is possible now to express the exponent of j_i in a much simpler form, viz., $\left[\sum_{i=0}^{m-1} yx^{iv} + \{mv\}_2 c \right]_1$. Such a statement will be justified when we have proved that

$$\sum_{i=0}^{m-2} r_{y,i} yx^{[iv]_2} + (yx^{p_2-v} + c) \sum_{i=0}^{m-3} s_{y,i} \sum_{j=i+1}^{m-2} r_{y,j} x^{[jv]_2 + (j-1-i)(p_2-v)} \prod_{f=i}^{j-1} s_{y,f} + yx^{[8m-1)v]_2} + x^{[(m-1)v]_2} \\ (yx^{p_2-v} + c) \sum_{i=0}^{m-2} x^{(m-2-i)(p_2-v)} \prod_{f=i}^{m-2} s_{y,f} + S_{y, m-1} c \equiv \sum_{i=0}^{m-1} yx^{iv} + \{mv\}_2 c \pmod{p_1}.$$

We can write

$$yx^{iv} = yx^{[iv]_2} + \{iv\}_2 p_2 = x^{[iv]_2}. yx^{\{iv\}_2 p_2}.$$

Then in view of (8),

$$yx^{iv} \equiv yx^{[iv]_2} \pmod{p_1}.$$

For every value of i from 0 to $m-3$ a typical term of the left member of the congruence is

$$r_{y,i} yx^{[iv]_2} + (yx^{p_2-v} + c) \left[s_{y,i} \sum_{j=i+1}^{m-2} r_{y,j} x^{[jv]_2 + (j-1-i)(p_2-v)} \prod_{f=i}^{j-1} s_{y,f} + x^{[(m-1)v]_2 + (m-2-i)(p_2-v)} \prod_{f=i}^{m-2} s_{y,f} \right].$$

If $r_{y,i} = 1$, then $s_{y,i} = 0$, and every thing vanishes except $yx^{[iv]_2}$ which we proved above to be congruent to its corresponding term in the right member. If, however, $r_{y,i} = 0$, then $s_{y,i} = 1$, and the quantity in the brackets is the part to be considered. Either $s_{y,i} = s_{y,i+1} = \dots = s_{y, m-2} = 1$ or some s , say $s_{y, i+k}$ ($i < i+k \leq m-2$), is zero. If the first condition prevails, the corresponding r 's are zero, and the last term in the brackets is the only one not to vanish. Leaving the c as a multiplier to be considered later, we must prove that

$$yx^{[(m-1)v]_2 + (m-1-i)(p_2-v)} \equiv yx^{iv} \pmod{p_1}.$$

As shown before, we may remove the $[\]_2$ from the first part of

the exponent without altering the congruence. After multiplying out and recombining, it becomes

$$yx^{(m-1-i)p_1 + iv} \equiv yx^{iv} \pmod{p_1}.$$

This is true at once from (8).

If, however, $s_{v,i+k} = 0$, then $r_{v,i+k} = 1$. We may say that this is the first s of those mentioned above to vanish; and hence the successive s 's from s_i to s_{i+k-1} are one, and the corresponding r 's are zero. Then the only part which does not vanish is

$$yx^{p_1-v} s_{v,i} r_{v,i+k} x^{[(i+k)v]_2 + (k-1)(p_1-v) \prod_{f=i}^{i+k-1} s_{v,f}}.$$

We need to show in this instance that

$$yx^{[(i+k)v]_2 + k[p_1-v]} \equiv yx^{iv} \pmod{p_1}.$$

This is true in the same way as in the preceding case.

We have yet to consider $i = m-2, m-1$. The $(m-2)$ th term is

$$r_{v,m-2} yx^{[(m-2)v]_2} + x^{[(m-1)v]_2} (yx^{p_1-v} + 0) s_{v,m-2}.$$

Disregarding c , this term is congruent to $yx^{(m-2)v}$, modulo p_1 , whether $r_{v,m-2}$ or $s_{v,m-2}$ is one. The only remaining term, $yx^{[(m-1)v]_2}$, needs but the usual modification, modulo p_1 , to be the same as $yx^{(m-1)v}$.

Terms with c as multiplier occur only when $s_{v,i} = 1$. There is one and only one term for every $s_{v,i} = 1$. In each case c is multiplied by some power of x ; but since $c \equiv \alpha x^s \pmod{p_1}^1$, where s is any positive integer, we may say that the terms in c amount to $c \sum_{i=0}^{m-1} s_{v,i}$. This is the same as $c \{mv\}_2$.

If we make the definitions

1. See (9).

$$\mathbb{Q}_m = M_0 M_1 \dots M_{m-1} \overline{M}_{m-1},$$

$$D_m = \sum_{i=0}^{m-1} y x^{i v} + \{m v\}_2 c,$$

then the powers of j'_1 in their final form are

$$(30) \quad (j'_1)^m = \mathbb{Q}_m j_1^{[D_m]}, j_2^{[m v]_2}.$$

The corresponding formulas for $(j'_2)^m$ are found in exactly the same manner. It will not be necessary to repeat the argument. The results are given below:

If we replace α by $\mathcal{A}$, v by z , and y by w , the quantities $s_{y,k}, \lambda_{y,k}, r_{y,k}, \xi_{y,k}, \eta_{y,k}, j_{y,k}, X_{y,k}, T_{y,k}, W_{y,k}, \overline{M}_k, \overline{M}_{m-1}, \mathbb{Q}_m, D_m$ become $s_{z,k}, \lambda_{z,k}, r_{z,k}, \xi_{w,k}, \eta_{w,k}, j_{w,k}, X_{w,k}, T_{w,k}, W_{w,k}, L_k, \overline{L}_{m-1}, \Lambda_m, E_m$, respectively. Then

$$(31) \quad (j'_2)^m = \Lambda_m j_1^{[E_m]}, j_2^{[m z]_2}.$$

The relation $(22)_1$ may now be written

$$\mathbb{Q}_m j_1^{[D_m]} j_2^{[m v]_2} = g(\psi_3).$$

In view of (15), the exponents of j_1 and j_2 are zero and the associativity condition is

$$(32) \quad \mathbb{Q}_m = g(\psi_3).$$

Likewise, $(22)_2$ is

$$\Lambda_{p_2} j_1^{[E_{p_2}]} j_2^{[p_2 z]_2} = \rho(\psi_3) \mathbb{Q}_c j_1^{[D_c]} j_2^{[c v]_2}.$$

Since from (10)₁, $p_2 z - c v$ is divisible by p_2 , and since $p_2 z$ is obviously divisible by p_2 , then $c v$ must also have p_2 as a factor. Hence $[c v]_2 = [p_2 z]_2 = 0$. Also $\{p_2 z\}_2 - \{c v\}_2 = \{p_2 z - c v\}_2$. Using these results in connection with (10), we see that the exponent of j_1 in the right member of the above equation equals that of j_1 in the left member. Hence the condition $(22)_2$ takes the form

$$(33) \quad \Lambda_{p_2} = \rho(\psi_3) \mathbb{Q}_c.$$

Now the condition (23) may be written

$$\delta j_1^w j_2^z \propto j_1^4 j_2^v = \beta(\psi_3) \otimes_\times j_1^{[D_1]} j_2^{[xv]_2} \delta j_1^w j_2^z.$$

Using (26) to transfer powers of j_2 past powers of j_1 , and then reducing exponents of j_1 and j_2 , modulo p_1 and p_2 , respectively, we get finally

$$\delta \alpha [\psi_2^z (\psi_1^w)] B_{\alpha, y} (\psi_1^w) q^{\{G'\}} (\rho (\psi_1^{[w+yx^2]_1})^{\{z+v\}_2} j_1^{[G']_1} j_2^{[z+v]_2} \beta(\psi_3) \otimes_\times \delta \\ [\psi_2^{[xv]_2} (\psi_1^{[D_1]_1})] B_{[xv]_2, w} (\psi_1^{[D_1]_1}) q^{\{G''\}} (\rho (\psi_1^{[1+wx^{[xv]_2]}]_1})^{\{[xv]_2+z\}_2} j_1^{[G'']_1} j_2^{[xv+z]_2},$$

where

$$G' = w + [yx^2]_1 + \{z+v\}_2 \text{ c } , \\ G'' = [D]_1 + [wx^{[xv]_2}]_1 + \{[xv]_2 + z\}_2 \text{ c } .$$

It is clear from (14), that the exponents of j_2 are equal. The exponents of j_1 will be the same if $G' \equiv G'' \pmod{p_1}$, or, stated in full, if

$$\sum_{i=0}^{x-1} yx^{iv} + \{xv\}_2 \text{ c } + wx^{[xv]_2} + \{[xv]_2 + z\}_2 \text{ c } - w - yx^2 - \{z+v\}_2 \text{ c } \equiv 0 \pmod{p_1}.$$

As brought out in an earlier part of this paper, $wx^{[xv]_2}$ may be replaced by wx^{xv} in a congruence with p_1 as modulus. Hence the only thing needed to make this congruence the same as (14)₂ is to prove that

$$\{xv\}_2 + \{[xv]_2 + z\}_2 - \{z+v\}_2 = \{xv-v\}_2.$$

The first two terms can be combined at once, and the statement in question becomes

$$\{xv+z\}_2 - \{z+v\}_2 = \{xv-v\}_2.$$

Since $z < p_2$ and $v < p_2$, then $\{z+v\}_2$ is either zero or one.

Since $xv-v$ is exactly divisible by p_2 , then

$$\{xv+z\}_2 = \begin{matrix} \{xv-v\}_2 \\ \text{or} \\ \{xv-v\}_2 + 1 \end{matrix}, \text{ according as } \{z+v\}_2 = \begin{matrix} 0 \\ \text{or} \\ 1 \end{matrix}.$$

In either case the above equality is established. This, in turn, establishes the desired congruence. Hence, the associativity condition in its final form is

$$(34) \quad \sigma \alpha [\psi_2^z (\psi_1^w)] B_{z,y} (\psi_1^w) g \{G'\}_1 (\rho (\psi_1^{[w+yx^z]_1})) \{z+v\}_2 = \beta (\psi_1) \otimes_x \sigma$$

$$[\psi_2^{[yv]_2} (\psi_1^{[D_1]_1})] B_{[yv]_2, w} (\psi_1^{[D_1]_1}) g \{G''\}_1 (\rho (\psi_1^{[D_1 + wx^{[xv]_2]}_1])) \{[xv]_2 + z\}_2,$$

where G' and G'' are defined earlier in this paragraph.

The requirement $(\mathcal{A}\beta)' = \mathcal{A}'\beta'$ has yielded the three associativity conditions, (32), (33), and (34).

We turn now to a new requirement, viz., $\gamma' = \gamma$, where $\gamma = \sigma j_1^{e_1} j_2^{e_2}$. Substituting from (20), (30), and (31), the condition becomes

$$\sigma (\psi_1) \otimes_{e_1} j_1^{e_1} j_2^{e_2} \Lambda_{e_2} [D_{e_1}]_1 [e, v]_2 [E_{e_2}]_1 [e, z]_2 = \sigma j_1^{e_1} j_2^{e_2}.$$

After transferring $j_2^{[e, v]_2}$ past $j_1^{[E_{e_2}]_1}$, combining powers of j_1 , and likewise powers of j_2 , and reducing them, modulo p_1 and p_2 , respectively, we get

$$\sigma (\psi_1) \otimes_{e_1} \Lambda_{e_2} [\psi_2^{[e, v]_2} (\psi_1^{[D_{e_1}]_1})] B_{[e, v]_2, [E_{e_2}]_1} (\psi_1^{[D_{e_1}]_1}) g \{[D_{e_1}]_1 + [E_{e_2} x^{[e, v]_2}]_1 + [e, v]_2 + [e, z]_2\}_2 c_1$$

$$(\rho (\psi_1^{[D_{e_1} + E_{e_2} x^{[e, v]_2}]_1})) \{[e, v]_2 + [e, z]_2\}_2 [D_{e_1} + E_{e_2} x^{[e, v]_2}]_2 \{[e, v]_2 + [e, z]_2\}_2 c_1 j_2^{[e, v + e, z]_2} = \sigma j_1^{e_1} j_2^{e_2}.$$

We have to prove that

$$e_1 v + e_2 z \equiv e_2 \pmod{p_2},$$

$$D_{e_1} + E_{e_2} x^{[e, v]_2} + \{[e, v]_2 + [e, z]_2\}_2 c \equiv e, \pmod{p_1}.$$

These congruences follow at once from (11) if we remember, first, that $\{e_2 z\}_2 c \times [e, v]_2$ may be replaced by $\{e_2 z\}_2 c$ because of (9), and, second, that

$$\{e, v\}_2 + \{e_2 z\}_2 + \{[e, v]_2 + [e, z]_2\}_2 = \{e, v + e_2 z\}_2.$$

Since by (11)₁, $e_2 z + e, v - e_2$ is exactly divisible by p_2 , and since $e_2 < p_2$, then $\{e, v + e_2 z\}_2 = \{e, v + e_2 z - p_2\}_2$. The condition $\gamma' = \gamma$ in its final form is then

$$(35) \quad \sigma (\psi_1) \otimes_{e_1} \Lambda_{e_2} [\psi_2^{[e, v]_2} (\psi_1^{[D_{e_1}]_1})] B_{[e, v]_2, [E_{e_2}]_1} (\psi_1^{[D_{e_1}]_1}) g \{[D_{e_1}]_1 + [E_{e_2} x^{[e, v]_2}]_1 + [e, v]_2 + [e, z]_2\}_2 c_1$$

$$+ \{[e, v]_2 + [e, z]_2\}_2 c_1 (\rho (\psi_1^{[D_{e_1} + E_{e_2} x^{[e, v]_2}]_1})) \{[e, v]_2 + [e, z]_2\}_2 = \sigma.$$

The last requirement for Γ to be associative is that

$$\mathcal{A}^{(p_2)} = \gamma \mathcal{A} \gamma^{-1}, \text{ where } \mathcal{A}^{(k+1)} = (\mathcal{A}^{(k)})'.$$

This will follow for every $\mathcal{A}$ if proved for $\mathcal{A} = j_1$ and $\mathcal{A} = j_2$. Hence we seek $j_1^{(p_2)}$ and $j_2^{(p_2)}$.

In order to keep the notation uniform throughout the derivation of $j_1^{(p_2)}$, we shall write $j_1' = \alpha j_1^{b_1} j_2^{a_1}$.

$$\begin{aligned} \text{Then } j_1'' &= (\alpha j_1^{b_1} j_2^{a_1})' \\ &= \alpha (\psi_3) (j_1')^{b_1} (j_2')^{a_1} \\ &= \alpha (\psi_3) \otimes_{b_1 j_1} [D_{b_1}]_1 j_2^{[b_1 v]_2} \wedge_{a_1 j_1} [E_{a_1}]_1 j_2^{[a_1 z]_2}. \end{aligned}$$

If we transfer $j_2^{[b_1 v]_2}$ past $\wedge_{a_1 j_1} [E_{a_1}]_1$, and then reduce powers of j_1 and j_2 , modulo p_1 and p_2 , respectively, we have, finally,

$$(36) \quad j_1'' = \Omega_0 (\psi_3) \Omega_1 j_1^{[D_{b_1} + x^{[b_1 v]_2} E_{a_1} + \{[b_1 v]_2 + [a_1 z]_2\}_2]_1} j_2^{[b_1 v + a_1 z]_2},$$

where

$$\begin{aligned} \Omega_0 &= \alpha, \\ \Omega_1 &= \otimes_{b_1 \wedge a_1} [\psi_2^{[b_1 v]_2} (\psi_1^{[D_{b_1}]_1})] B_{[b_1 v]_2, [E_{a_1}]_1} (\psi_1^{[D_{b_1}]_1}) g^{\{[D_{b_1}]_1 + [x^{[b_1 v]_2} E_{a_1}]_1 + \{[b_1 v]_2 + [a_1 z]_2\}_2\}_1} \\ &\quad E_{a_1}]_1 + \{[b_1 v]_2 + [a_1 z]_2\}_2\}_1 (\rho (\psi_1^{[D_{b_1} + x^{[b_1 v]_2} E_{a_1}]_1}) \{[b_1 v]_2 + [a_1 z]_2\}_2). \end{aligned}$$

Since (8) enables us to replace $x^{[b_1 v]_2} b_1$ by $x^{b_1 v}$, and (9) to replace $x^{[b_1 v]_2} \{a_1 z\}_2 c$ by $\{a_1 z\}_2 c$, we may use the definitions given in (6) to simplify the exponents of j_1 and j_2 . Then j_1'' may be written as

$$(37) \quad j_1'' = \Omega_0 (\psi_3) \Omega_1 j_1^{[b_2 + \{a_1\}_2]_1} j_2^{[a_2]_2}.$$

By an induction on r , we shall prove that

$$(38) \quad j_1^{(r)} = \Omega_0 (\psi_3^{r-1}) \Omega_1 (\psi_3^{r-2}) \dots \Omega_{r-2} (\psi_3) \Omega_{r-1} j_1^{[t_r]_1} j_2^{[a_r]_2},$$

where

$$\begin{aligned} t_r &= b_r + \{a_r\}_2 c, \\ \Omega_0 &= \alpha, \\ \Omega_k &= \otimes_{[t_k]_1} \wedge_{[a_k]_2} [\psi_2^{[t_k]_1 v]_2} (\psi_1^{[D_{[t_k]_1}]_1})] B_{[t_k]_1 v]_2, [E_{[a_k]_2}]_1} (\psi_1^{[D_{[t_k]_1}]_1}) \\ &\quad g^{\{[D_{[t_k]_1}]_1 + [E_{[a_k]_2}]_1 x^{[t_k]_1 v]_2} + \{[t_k]_1 v]_2 + [a_k z]_2\}_2\}_1} (\rho (\psi_1^{[D_{[t_k]_1} + E_{[a_k]_2}]_1} x^{[t_k]_1 v]_2} j_1) \{[t_k]_1 v]_2 + [a_k z]_2\}_2). \end{aligned}$$

The value of j_1'' , as given by (38) with $r = 2$, agrees with that of (37), if we can but show that Ω_1 as given in (36) is the same as Ω_k for $k \geq 1$. This follows at once if we remember that $a_1 = v < p_2$, $b_1 = y < p_1$, and hence $[b_1 + \{a_1\}_2 c]_1 = b_1$, while $[a_1]_2 = a_1$. To make the computation as simple as possible we use the definition

$$(39) \quad \Xi_r = \Omega_0(\psi_3^{r-1}) \Omega_1(\psi_3^{r-2}) \dots \Omega_{r-2}(\psi_3) \Omega_{r-1};$$

and the temporary abbreviations

$$(40) \quad \begin{aligned} [t_r]_1 &= p, & [a_r]_2 &= q. \\ j_1^{(r)} &= \Xi_r j_1^p j_2^q, \text{ and} \\ j_1^{(r+1)} &= \Xi_r (\psi_3) (j_1')^p (j_2')^q \\ &= \Xi_r (\psi_3) \otimes_p j_1^{[D_p]_1} j_2^{[p_v]_2} \wedge_q j_1^{[E_q]_1} j_2^{[q_z]_2}. \end{aligned}$$

After transferring $j_2^{[p_v]_2}$ past $j_1^{[E_q]_1}$, we combine powers of j_1 and likewise powers of j_2 . If we then use (17), and (17)₂ to reduce them modulo p , and p_2 , respectively, the following result is obtained:

$$(41) \quad j_1^{(r+1)} = \Xi_r (\psi_3) \otimes_p \wedge_q [\psi_2^{[p_v]_2} (\psi_1^{[D_p]_1})] B_{[p_v]_2, [E_q]_1} (\psi_1^{[D_p]_1}) q^{\{[D_p]_1 + [E_q]_1^{[p_v]_2}\}_1} \\ + \{[p_v]_2 + [q_z]_2\}_2 c_1 (\rho(\psi_1^{[D_p]_1 + E_q x^{[p_v]_2}} j_1)) \{[p_v]_2 + [q_z]_2\}_2 \cdot [D_p x^{[p_v]_2} + \{[p_v]_2 + [q_z]_2\}_2 c_1] \cdot j_2^{[p_v + q_z]_2}$$

If we replace p and q by their values from (40), we see that the factors $\otimes \wedge B g \rho$ of (41) are exactly Ω_r ; and, hence, except for the exponents of j_1 and j_2 , (41) is exactly the same as (38) with r replaced by $r+1$. Therefore, all we need to complete the induction is to prove that

$$(42) \quad \begin{cases} [b_r + \{a_r\}_2 c]_1 v + [a_r]_2 z \equiv a_{r+1} & (\text{mod } p_2), \\ [D_{b_r + \{a_r\}_2 c}]_1 + E_{[a_r]_2} x^{[b_r + \{a_r\}_2 c]_1 v} + \{[b_r + \{a_r\}_2 c]_1 v\}_2 + [a_r]_2 z \equiv b_{r+1} + \{a_{r+1}\}_2 c & (\text{mod } p_1). \end{cases}$$

To establish (42), we replace $[b_r + \{a_r\}_2 c]_1$ and a_{r+1} by their equals $b_r + \{a_r\}_2 c - \{b_r + \{a_r\}_2 c\}_1 p_1$ and $a_r z + b_r v$. The con-

gruence then takes the form

$$b_r v + \{a_r\}_z cv - \{b_r + \{a_r\}_z c\}, p_1 v + \{a_r\}_z z \equiv a_r z + b_r v \pmod{p_2}.$$

Obviously $\{a_r\}_z$ may be replaced by a_r . From (10), we see that $cv \equiv 0 \pmod{p_2}$. This fact, with (15), establishes the truth of (42)₁.

The proof of (42)₂ is somewhat longer. According to the argument in the preceding paragraph,

$$x^{[b_r + \{a_r\}_z c]_1 v}_z = x^{[b_r v]_z}.$$

Due to (8), $x^{[b_r v]_z}$ may be replaced by $x^{b_r v}$ in this congruence.

After substituting for $E_{[a_r]_z}$ and $D_{[b_r + \{a_r\}_z c]_1}$ their values from (31) and (30), we may, because of (9), replace $\{[a_r]_z z\}_2 c x^{b_r v}$ by $\{[a_r]_z z\}_2 c$. Then, if we combine this with the other two terms in c which appear on the left, and substitute on the right for a_{r+1} and b_{r+1} their values in terms of a_r and b_r as given in

(6), (42)₂ takes the form

$$(43) \quad \sum_{i=0}^{[b_r + \{a_r\}_z c]_1 - 1} y x^{iv} + x^{b_r v} \sum_{i=0}^{[a_r]_z - 1} w x^{iz} + \{[b_r + \{a_r\}_z c]_1 v + [a_r]_z z\}_2 c \\ \equiv x^{b_r v} \sum_{i=0}^{a_r - 1} w x^{iz} + \sum_{i=0}^{b_r - 1} y x^{iv} + \{a_r z + b_r v\}_2 c \pmod{p_1}.$$

We notice that

$$x^{b_r v} \sum_{i=0}^{a_r - 1} w x^{iz} - x^{b_r v} \sum_{i=0}^{[a_r]_z - 1} w x^{iz} = x^{b_r v} \sum_{i=[a_r]_z}^{a_r - 1} w x^{iz} = \sum_{i=[a_r]_z}^{a_r - 1} w x^{iz + b_r v}.$$

Due to (8), the values of $w x^{iz + b_r v}$ repeat themselves, modulo p_1 , after p_2 of them have been used. Hence

$$\sum_{i=[a_r]_z}^{a_r - 1} w x^{iz + b_r v} \equiv \{a_r\}_z \sum_{i=0}^{p_2 - 1} w x^{iz} \pmod{p_1}.$$

Due to the fact that $p_1 v \equiv 0 \pmod{p_2}$, we may use (7) and write

$$\sum_{i=0}^{b_r + \{a_r\}_z c - 1} y x^{iv} \equiv \sum_{i=0}^{[b_r + \{a_r\}_z c]_1 - 1} y x^{iv} + \{b_r + \{a_r\}_z c\}_1 \sum_{i=0}^{p_1 - 1} y x^{iv} \pmod{p_1}.$$

Hence in (43) the two terms $\sum_{i=0}^{[b_r + \{a_r\}_z c]_1 - 1} y x^{iv} - \sum_{i=0}^{b_r - 1} y x^{iv}$ may be replaced by

$$\sum_{i=b_r}^{b_r + \{a_r\}_z c - 1} y x^{iv} - \{b_r + \{a_r\}_z c\}_1 \sum_{i=0}^{p_1 - 1} y x^{iv}.$$

Due to the fact that $cv \equiv 0 \pmod{p_2}$, the terms of the first $\sum$

repeat themselves after c terms have been used, modulo p_1 , and the difference of the 2 $\sum$'s can finally be replaced by

$$\{a_r\}_z \sum_{i=0}^{c-1} yx^{iv} - \{b_r + \{a_r\}_z c\}_1 \sum_{i=0}^{h_1-1} yx^{iv}.$$

If we make these replacements in (43), and also change the terms in c to a different form, we have

$$(44) \quad \{a_r\}_z x^{b_r v} \sum_{i=0}^{p_1-1} wx^{iz} - \{a_r\}_z \sum_{i=0}^{c-1} yx^{iv} + \{b_r + \{a_r\}_z c\}_1 \sum_{i=0}^{h_1-1} yx^{iv} \\ + \frac{a_r z + b_r v}{c} - \frac{[a_r z + b_r v]_z}{c} - \frac{[b_r + \{a_r\}_z c]_1 v + [a_r]_z z}{c} \\ + \frac{[b_r + \{a_r\}_z c]_1 v + [a_r]_z z}{c} \equiv 0 \pmod{p_1}.$$

From (42)₁, which we have already established, we see that the numerators of the second and fourth fractions are equal, and hence their difference is zero. The other two fractions may be rewritten as

$$\frac{a_r z + b_r v - \{b_r + \{a_r\}_z c\}_1 v + \{b_r + \{a_r\}_z c\}_1 p_1 v - [a_r]_z z}{p_2} c$$

Combining terms, we have

$$\frac{\{a_r\}_z p_2 z - \{a_r\}_z cv + \{b_r + \{a_r\}_z c\}_1 p_1 v}{p_1} c.$$

Since $p_2 z - cv$ and $p_1 v$ are each exactly divisible by p_2 , this can be expressed as

$$\{a_r\}_z \{p_2 z - cv\}_2 c + \{b_r + \{a_r\}_z c\}_1 \{p_1 v\}_2 c.$$

Substituting this in (44), we have

$$\{a_r\}_z \sum_{i=0}^{p_2-1} wx^{iz} - \{a_r\}_z \sum_{i=0}^{c-1} yx^{iv} + \{a_r\}_z \{p_2 z - cv\}_2 c \\ + \{b_r + \{a_r\}_z c\}_1 \sum_{i=0}^{p_1-1} yx^{iv} + \{b_r + \{a_r\}_z c\}_1 \{p_1 v\}_2 c \equiv 0 \pmod{p_1}.$$

It is clear from (10)₂ and (15)₂ that this congruence is true.

Hence (42)₂ is established and the induction is complete.

Then we may say

$$(45) \quad j_1^{(p_2)} = \frac{1}{p_2} j_1 [b_{p_2} + \{a_r\}_z c]_1 \quad j_z^{[a_r]_2}.$$

We may go through exactly the same argument and derive the

formula

$$(46) \quad j_z^{(p_3)} = \pi_{p_3} \quad j_1^{[d_{p_3} + \{f_{p_3}\}_2 c]_1} \quad j_2^{[f_{p_3}]_2} ,$$

where

$$\pi_{p_3} = \Delta_0 (\psi_3^{p_3-1}) \Delta_1 (\psi_3^{p_3-2}) \dots \Delta_{p_3-1} (\psi_3) \Delta_{p_3} ,$$

$$\Delta_0 = \delta , \quad u_k = d_k + \{f_k\}_2 c ,$$

$$\Delta_k = \bigotimes_{[u_k]_1} \wedge_{[f_k]_2} [\psi_z^{[u_k]_1 v}]_z (\psi_1^{[D_{[u_k]_1}]_1}) B_{[u_k]_1 v]_2, [E_{[f_k]_2}]} (\psi_1^{[D_{[u_k]_1}]_1}) \\ g^{\{[D_{[u_k]_1}]_1 + [x^{[u_k]_1 v}]_2 E_{[f_k]_2}]_1 + \{[u_k]_1 v\}_2 + \{f_k\}_2 c\}} (\psi_1^{[D_{[u_k]_1}]_1 + x^{[u_k]_1 v]_2 E_{[f_k]_2}]_1}) \{[u_k]_1 v\}_2 + \{f_k\}_2\}_2$$

We shall deal first with the condition $j_1^{(p_3)} = \gamma j_1 \gamma^{-1}$,

where $\gamma = \sigma j_1^{e_1} j_2^{e_2}$. Substituting from (45) for $j_1^{(p_3)}$, and multiplying both members of the equation on the right by γ , we get

$$\equiv_{p_3} j_1^{[b_{p_3} + \{a_{p_3}\}_2 c]_1} j_2^{[a_{p_3}]_2} \sigma j_1^{e_1} j_2^{e_2} = \sigma j_1^{e_1} j_2^{e_2} j_1 .$$

After transferring powers of j_2 past powers of j_1 in both members and performing the customary simplification, this becomes

$$\equiv_{p_3} \sigma [\psi_z^{[a_{p_3}]_2} (\psi_1^{[b_{p_3} + \{a_{p_3}\}_2 c]_1})] B_{[a_{p_3}]_2, e_1} (\psi_1^{[b_{p_3} + \{a_{p_3}\}_2 c]_1}) \{[b_{p_3} + \{a_{p_3}\}_2 c]_1 + [e_1 x^{[a_{p_3}]_2}]_1\} \\ j_1^{[b_{p_3} + \{a_{p_3}\}_2 c + e_1 x^{[a_{p_3}]_2}]_1} j_2^{[a_{p_3}]_2 + e_2} = \sigma B_{e_2, 1} (\psi_1^{e_1}) q^{\{e_1 + [x^{e_2}]_1\}_1 \cdot [e_1 + x^{e_2}]_1} j_1^{e_1} j_2^{e_2} .$$

Since by (12) , $[a_{p_3}]_2 = 0$, the exponents of j_2 are equal. The use of (12) , again, together with (12)₂ , shows the exponents of j_1 equal. The condition finally becomes

$$(47) \equiv_{p_3} \sigma (\psi_1^{[b_{p_3} + \{a_{p_3}\}_2 c]_1}) q^{\{[b_{p_3} + \{a_{p_3}\}_2 c]_1 + e_1\}_1 - \{e_1 + [x^{e_2}]_1\}_1} = \sigma B_{e_2, 1} (\psi_1^{e_1}) .$$

Likewise, the condition that $j_2^{(p_3)} = \gamma j_2 \gamma^{-1}$ becomes

$$\pi_{p_3} j_1^{[d_{p_3} + \{f_{p_3}\}_2 c]_1} j_2^{[f_{p_3}]_2} \sigma j_1^{e_1} j_2^{e_2} = \sigma j_1^{e_1} j_2^{e_2+1} .$$

After the usual simplifications, this takes the form

$$\pi_{p_3} \sigma [\psi_z^{[f_{p_3}]_2} (\psi_1^{[d_{p_3} + \{f_{p_3}\}_2 c]_1})] B_{[f_{p_3}]_2, e_1} (\psi_1^{[d_{p_3} + \{f_{p_3}\}_2 c]_1}) q^{\{[d_{p_3} + \{f_{p_3}\}_2 c]_1 + [e_1 x^{[f_{p_3}]_2}]_1\}_1} \\ j_1^{[d_{p_3} + \{f_{p_3}\}_2 c + e_1 x^{[f_{p_3}]_2}]_1} j_2^{[f_{p_3}]_2 + e_2} = \sigma j_1^{e_1} j_2^{e_2+1} .$$

Since by (13) , $f_{p_3} - 1 \equiv 0 \pmod{p_2}$, then $[f_{p_3}]_2 = [f_{p_3} - 1]_2$. Also, as before, $x^{[f_{p_3}]_2} \equiv x^{f_{p_3}} \pmod{p_1}$, and hence may be replaced by it. Then the congruences (13) show the exponents of the j_2 's to be equal and also those of the j_1 's. Then the condition in its

final form, after replacing $[f_{p_3}]_2$ by 1, is

$$(48) \prod_{p_3} \sigma[\psi_2(\psi_1^{[d_{p_1} + \{f_{p_1}\}_2 c]_1})] \beta(\psi_1^{[d_{p_1} + \{f_{p_1}\}_2 c]_1}) q^{\{[d_{p_1} + \{f_{p_1}\}_2 c]_1 + [e, v]_1\}} = \sigma$$

We have now proved the following

Theorem. Let $f(x) = 0$ be an equation of degree $n = p_1 p_2 p_3$, irreducible in a field F , whose group for F is generated by three generators ψ_1, ψ_2, ψ_3 , as given by (1) and (2). The algebra Γ , composed of all polynomials in i, j_1, j_2 , and j_3 , is associative if, and only if, conditions (32), (33), (34), (35), (47), and (48) hold in addition to the four conditions¹ that the subalgebra Σ be associative.

1. Dickson, Transactions of the American Mathematical Society, Vol. 32, (1930), pp. 319-34.

VITA

Dora McFarland was born April 18, 1895, near Aledo, Illinois. She attended grade and high school at Aledo and subsequently Monmouth College at Monmouth, Illinois, where she graduated in 1916. She taught for some years in Illinois high schools and during summers attended the University of Oklahoma, Norman, Oklahoma, where she was granted a degree of Master of Arts in 1921. Since 1920 she has been connected with the mathematics staff of the University of Oklahoma. During 1924-25 and again during 1928-29, she attended the University of Chicago where she studied under Professors Moore, Slaught, Dickson, Bliss, MacMillan, Lane, Logsdon, Bartky, Bell and Coble. This paper was prepared under the direction of Professor L. E. Dickson to whom, at this time, grateful acknowledgment is made for his kindly interest and guidance.

